REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

WILMER CUTLER PICKERING HALE AND DORR LLP
SONAL N. MEHTA (SBN 222086)
sonal.mehta@wilmerhale.com
THOMAS G. SPRANKLING (SBN 294831)
thomas.sprankling@wilmerhale.com
JOSEPH M. LEVY (SBN 329318)
joseph.levy@wilmerhale.com
2600 El Camino Real, Suite 400
Palo Alto, CA 94306
Telephone: (650) 858-6000

ARI HOLTZBLATT (*pro hac vice* pending)
Ari.Holtzblatt@wilmerhale.com
ALLISON SCHULTZ (*pro hac vice* pending)
Allison.Schultz@wilmerhale.com
ROBIN C. BURRELL (*pro hac vice* pending)
robin.burrell@wilmerhale.com
1875 Pennsylvania Ave, NW
Washington, DC 20006
Telephone: (202) 663-6000
Facsimile: (202) 663-6363

Attorneys for Plaintiff
Facebook, Inc.

HUNTON ANDREWS KURTH LLP
Ann Marie Mortimer (State Bar No. 169077)
amortimer@HuntonAK.com
Jason J. Kim (State Bar No. 221476)
kimj@HuntonAK.com
Jeff R. R. Nelson (State Bar No. 301546)
jnelson@HuntonAK.com
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627
Telephone: (213) 532-200
Facsimile: (213) 532-2020

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FACEBOOK, INC., a Delaware corporation,
Plaintiff,

v.

BRANDTOTAL LTD., an Israeli corporation, and UNIMANIA, INC., a Delaware corporation,
Defendants.

Case No. 3:20-CV-07182-JCS

PLAINTIFF FACEBOOK INC.'S OPPOSITION TO DEFENDANTS' *EX PARTE* APPLICATION FOR TEMPORARY RESTRAINING ORDER

Hon. Joseph C. Spero
Courtroom F – 15th Floor
Date: October 26, 2020
Time: 2:00 p.m.

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF CONTENTS

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF AUTHORITIES

Page(s)

CASES

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

DOCKETED CASES

STATUTES, RULES, AND REGULATIONS

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

OTHER AUTHORITIES

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

Defendants BrandTotal, Ltd. and Unimania, Inc. ("Defendants" or "BrandTotal") built their business by harvesting data from Facebook, in violation of Facebook's Terms of Service. To facilitate their data harvesting activities, Defendants developed and distributed internet browser extensions on the Google Chrome Web Store, as well as a mobile application, all designed and programed to scrape[1] data from Facebook and other sites. To conceal their scraping from Facebook's systems, Defendants used the browser of any anyone who installed their extension as a proxy to access Facebook and engage in automated extraction of data to servers Defendants controlled. The data Defendants scraped included user profile information, advertisements and advertisement metrics, and user advertisement interest information. Not only was this data scraped from password-protected locations on Facebook, but some of the data was non-public. Defendants' misconduct was a clear breach of Facebook's Terms of Service, to which Defendants agreed, and violated federal and state law as alleged in the Complaint. Defendants' conduct also put the security and integrity of Facebook and its users at risk. Now, after Facebook discovered that Defendants used several tools to scrape from Facebook, Defendants ask the Court to issue a ***mandatory injunction*** to regain access to Facebook password-protected computers and information they never should have had in the first place. This is not relief that should be granted at all, let alone on a request for temporary restraining order ("TRO").

At the outset, there is no dispute that Defendants are asking for an order compelling action by a party that cannot repair the alleged irreparable injury. While Facebook can reinstate Defendants' Facebook accounts, reinstating those accounts would not restore the functionality that Defendants claim they need. For that, Defendants need their browser extension reinstated on the Google Chrome Web Store. But Facebook ***does not control*** the Google Chrome Web Store. Thus, as Defendants acknowledge, even if this Court grants the emergency relief requested, "this only means the Court will be ordering Facebook to contact Google to withdraw its request to have UpVoice taken down." Defendants' Resp. to Plaintiff's Admin. Mtn. to Set Briefing Schedule (Dkt. No. 29) at 3. "There is no telling how quickly Google will respond" and "if Google does not respond, BrandTotal ***may have to file an action to seek a TRO against Google***." *Id.* at 3.[2] In other words, Defendants admit that

[1] Data scraping is the automated extraction of user data. *See* Declaration of Mike Clark ISO Facebook Opp. To TRO ("Clark Decl.") ¶ 3.

[2] Emphasis supplied and internal citations omitted, unless otherwise noted.

Facebook is not itself able to cure the alleged injury. The TRO should be denied on that basis alone.

In any case, even if Facebook did have the ability to address the alleged injury here, Defendants have not established that the extraordinary relief of a TRO is warranted. At its core, Defendants' argument is that they have the absolute right to collect data from Facebook users. Defendants do not identify any case in which a court has restored a data scraper's access to a platform even after it engaged in the unauthorized collection of user data and abuse of the platform's products and systems. The best Defendants can muster is the Ninth Circuit's decision in *hiQ v. LinkedIn*, which Defendants contend is "on all fours" with the instant case.

hiQ in no way supports Defendants' extraordinary claim. To start, *hiQ* expressly encouraged "victims of data scraping" to bring breach of contract actions to protect their rights—precisely as Facebook has done here. *hiQ v. LinkedIn,* 938 F.3d 985, 1004 (9th Cir. 2019). And there are dispositive differences between the data scraping addressed in hiQ and the scraping here. Most significant is that, unlike the data scraped in *hiQ*, ***all*** of the information scraped by Defendants was obtained through password-protected channels. This allowed Defendants to ride on the coattails of a user to enter a password-protected location and collect data, all without permission from Facebook or any other user whose information they might obtain. There is no reading of *hiQ* that would allow a company to exploit login credentials of individual users to enter password-protected locations of the Facebook platform to collect ads (and information and metrics about those ads) without the consent or knowledge of Facebook or the advertisers who created and published them.

hiQ itself confirms that. In the context of the Computer Fraud and Abuse Act ("CFAA"), the *hiQ* Court drew an express, and essential, distinction between the scraping of information from publicly-accessible locations on a website and information from password-protected locations on the website. *Id.* at 1002 (citing *Facebook, Inc. v. Power Ventures*, 844 F.3d 1058, 1067 n.2 (9th Cir. 2016)). As *hiQ* itself acknowledged, it is the Ninth Circuit's earlier decision in *Power Ventures* that "control[s] situations in which authorization generally is required and has either never been given or has been revoked." *See hiQ*, 938 F.3d at 1002. "While Power Ventures was gathering user data that was protected by Facebook's username and password authentication system [as Defendants do here], the data hiQ was scraping was available to anyone with a web browser [as Defendants do not even

claim to be doing here]." *Id.* Although Defendants invoke *hiQ* no fewer than a dozen times, they fail to even cite—let alone confront—*Power Ventures*.

Nor do they reckon with—or even recognize—Chief Judge Hamilton's ruling last year in the *Stackla v. Facebook* TRO proceedings. *Stackla, Inc. v. Facebook*, 2019 WL 4738288 (N.D. Cal. Sept. 27, 2019). As here, the movant in *Stackla* asked the court to grant a TRO that would sanction their automated collection of user data in violation of Facebook's terms, which they claimed was necessary for them to continue to offer advertising and marketing services to their customers. And as here, the implications of such a ruling would have been significant. As the *Stackla* Court recognized, "the public has a strong interest in the integrity of Facebook's platforms, Facebook's policing of those platforms for abuses, and Facebook's protection of its users' privacy." 2019 WL 4738288, at *6. Companies who violate Facebook's policies cannot just show up at the courthouse steps and demand that their access be reinstated. "Although the public certainly has some interest in avoiding the dissolution of companies and the accompanying loss of employment, Facebook's ability to decisively police the integrity of its platforms is without question a pressing public interest." *Id.*

That the balance of hardships strongly disfavors a temporary restraining order is confirmed by Defendants' anemic showing on the irreparable injury prong. Defendants claim that their business will be destroyed without a TRO, but Defendants offer no evidence of any imminent injury beyond generalized averments from the company's CEO that the company "cannot long survive." This is simply not enough to warrant emergency relief. As the *Stackla* Court explained, "the extraordinary relief of a pre-adjudicatory injunction demands more precision with respect to when irreparable harm will occur than 'soon.'" 2019 WL 4738288, at *5. And while Defendants suggest that customers and investors are considering the lawsuit and speculate that they will ultimately lose business as a result, the *Stackla* Court rejected this precise argument on the grounds that mere customer "concerns … does not demonstrate a likelihood that they will cease paying" the Defendants—"much less that they will do so imminently." *Id.* at *4. Ultimately, Defendants never explain how a company boasting millions in funding (including $12 million in funding just last month) and A-list customers can claim to be on the verge of imminent bankruptcy.

If the Court were to reach the question of likelihood of success on the merits (it need not), that

factor would only confirm that emergency relief should be rejected. Defendants fail to plead—let alone persuasively establish—facts supporting their own counterclaims. As one example, Defendants argue they will likely win on intentional interference with prospective economic advantage but fail to adequately plead the basic elements of that claim, including that Facebook "knew about" and "intentionally disrupted" specific deals with Defendants' customers. *Buxton v. Eagle Test Sys. Inc.*, 2010 WL 1240749, at *2 (N.D. Cal. Mar. 26, 2010). A pleading that fails to allege even basic requirements of the claims is not one on which a party can credibly ask for emergency relief. Defendants' showing of a likelihood of success in defending against Facebook's affirmative claims fares no better. For example, Defendants' *only* response to Facebook's allegations that Defendant have violated the CFAA and California Penal Code § 502 ("Section 502") is that the information they scrape is "public." But Facebook has alleged, and establishes through sworn declarations submitted herewith, that Defendants are scraping information without authorization through password-protected channels, not public channels. In other words, Defendants will not prevail on Facebook's claims or their own. The motion for temporary restraining order should be denied.

I. FACTUAL BACKGROUND

Browser extensions are small computer programs that add functionality to users' web browsers. Sometimes browser extensions can add features to a user's web browser experience such as blocking pop-up ads. *See* Declaration of Sanchit Karve ISO Facebook Opp. To TRO ("Karve Decl.") ¶ 9. Other times, browser extensions can be used for malicious purposes, such as spying or data theft. *Id.* ¶ 10. Google allows developers to create extensions for the Google Chrome web browser and to distribute those extensions though the Google Chrome Web Store, and Google has its own terms of service that govern those transactions. *See* Declaration of Sonal Mehta ISO Facebook Opp. To TRO ("Mehta Decl."), Ex. 1 (https://developer.chrome.com/webstore/terms) at Section 4 ("4.4.1 You agree that you will not engage in any activity with the Web Store, including the development or publication of Products or other materials, that violates the Google Chrome Web Store Program Policies, or that: 1. knowingly violates a third party's terms of service; 2. violates any applicable laws or regulations, . . ."), Section 7 ("Product Takedowns, Review, and Updates").

Defendants have developed, distributed, and obtained data through at least six browser

extensions and an app designed to automatically collect data from Twitter, YouTube, LinkedIn, Amazon, Facebook, and Instagram. Declaration of Alon Leibovich ("Leibovich Decl.") (Dkt. 26-08) ¶ 6. The extensions were available for download through the Google Chrome Web Store. Karve Decl. ¶ 7. As of this filing, the Anonymous Story Viewer for Instagram app is still available for download on Google Play, Google's platform for distributing mobile and desktop apps. *Id*. Although each of Defendants' extensions and their app improperly rely on a user's login credentials to gain entry into password protected locations on Facebook's (or Instagram's) platform and thus conceal their scraping, the UpVoice extension (described below) is the only extension at issue in the TRO.

A. Defendants Contracted To Abide By Facebook's Terms

Data scraping is a serious concern for social-media platforms like Facebook. Clark Decl. ¶ 5. It circumvents measures employed by platforms to prevent unauthorized automated requests and thus makes sites less secure and more vulnerable to harmful acts; it can interfere with the operations and integrity of the platform's networks and security; it can degrade public trust and confidence in the platform; and more. *Id.* In July 2019, Facebook reached a settlement with the FTC including a consent decree ordering it to implement certain privacy protections to, among other things, report certain incidents of unauthorized collection or access to user data, *Id.* ¶ 12.

When creating an account, every Facebook and Instagram user must agree to the terms of service that govern each platform, including the Facebook Terms of Service and Facebook Commercial Terms (collectively, "Facebook Terms"), and the Instagram Terms of Use, Community Guidelines, and Platform Policy (collectively, "Instagram Terms and Policies"). *See* Declaration of Michael Duffey ISO Facebook Opp. To TRO ("Duffey Decl.") ¶¶ 3, 4. As relevant here, both the Facebook and Instagram terms prohibit "accessing or collecting information in an automated way." *See* Clark Decl. ¶ 7; Duffey Decl. Exs. 1-3.[3] Defendants agreed to abide by these terms, including the

[3] The Instagram Terms also prohibit users from "violat[ing] someone else's rights, including intellectual property rights." Duffey Decl. Ex. 3. In addition, the Instagram Terms and Section 3.2.1 of the Facebook Terms prohibit users from "do[ing] … anything unlawful, misleading, [ ] or fraudulent" or facilitating or supporting others in doing so." Duffey Decl. Exs. 1 & 3. And both the Instagram Terms and Section 3.2.2 of the Facebook Terms prohibits users from doing anything to impair the proper operation of the platforms. Duffey Decl. Exs. 1 & 3.

anti-scraping policies, by creating and maintaining their own Facebook and Instagram accounts between 2016 and October 2020. Karve Decl. ¶¶ 27-34; Duffey Decl. ¶¶ 3, 4.

B. Defendants Violated Facebook's Terms By Automatically Collecting Data

For years, Defendants exploited Facebook's users' access to Facebook and Instagram to scrape information from password-protected locations. So far, Facebook has identified at least six browser extensions and an app created by Defendants to scrape the platforms. Karve Decl. ¶¶ 5-6. For example, Defendants' Ads Feed extension collected demographic and advertising data without paying users. Compl. Ex. 9. The Anonymous Story Viewer for Instagram app, still available for download on Google Play as of this filing, scrapes an Instagram user's ID, name, phone number, email address, gender profile picture, Instagram accounts followed by the user and the name of the Instagram accounts following the user, the user's posts, and the comments and captions for posts, the URL for the posts, and the geotag of the Instagram post, which is information embedded in the metadata of the photo that shows where the photo in the post was taken. Karve Decl. ¶ 22. None of the information was anonymized. *Id.* The app was also coded to scrape the user's session token and the user's session ID. *Id.* ¶ 23. This information was exfiltrated to a third-party server as well. Anyone with the session token and session ID can use them to make requests to Facebook computers for Instagram content for that user without the user accessing Instagram. *Id.*

The UpVoice extension, which is the only extension Defendants address in their TRO, pays users for browsing the web while secretly collecting data. Karve Decl. ¶¶ 14-17 & Ex. 3. Once Defendants' UpVoice extension had been installed, the extension *automatically* collected data, including non-public data, from password-protected locations when the user visited Facebook. *Id.* ¶¶ 13-17. This creates a risk that whenever *anyone* using that browser—including family members or roommates using a shared computer—accesses Facebook (or another website Defendants targeted for scraping) they would unwittingly have their data scraped as well. Clark Decl. ¶ 5(c). Defendants' own public statements about the extension contradict their denial that it is automated. For example, in promoting UpVoice, Defendants emphasized that the extension requires nothing more of users than "browsing" what they misleadingly refer to as "participating sites" just "as [users] normally do." Karve Decl. Ex. 3. All users have to do is "regularly visit Facebook," and UpVoice works behind the scenes

to "collect the ads that you see and anonymous demographic profile data." *Id.* It accomplishes this by masquerading as an authenticated Facebook user with legitimate login credentials. Karve Decl. ¶ 15.

The UpVoice extension enabled Defendants to access password-protected locations and automatically collected ad and ***non-public*** user information in violation of Facebook's terms. It was coded to scrape information from the password-protected Facebook account of the Facebook user—including their Facebook user ID, gender, date of birth, relationship status, and location—as well as data about advertisements the user sees while browsing Facebook. *Id.* ¶ 15, 17(a)-(b). Facebook's privacy settings allow users to control how much profile information is viewable publicly, and a user's date of birth, relationship status, and location can be set to private or public. *Id.* ¶ 17(a). The extension scraped user profile information regardless of the privacy setting. *Id.* It was also coded to scrape data about the ads themselves, including the text of the ad, any images or videos used, and information about who sponsored the ad. *Id.* ¶ 17(c). It also scraped URLs associated with the ads, enabling them to compile a database of web addresses to permanent webpages that contain images of the ads. *Id.*

UpVoice also collected data on advertising metrics. *Id.* ¶ 17(d). Facebook users can engage with ads in various ways; beyond simply viewing ads, users can comment on them, react to them using various icons—including a thumbs-up, heart, or sad face—and share them with other Facebook users. *Id.* UpVoice scraped that data from a password-protected location, collecting information on how many comments, reactions, and shares an ad has.[4] *Id.* ¶¶ 15, 17(d).

In addition to advertising data, UpVoice also scraped users' advertising interests. Karve Decl. ¶ 17(b). Advertising interests are part of a users' Ad Preference information and they are not publicly viewable. *Id.* Ad interests are accessible to an authenticated Facebook user through their profile settings. *Id.* The UpVoice extension scraped users' advertising-interest categories from its password-

[4] Only registered Facebook users can create and place ads on the platform. Leathern Decl. ¶ 4. Ads belong to the users who created them, and often contain licensed copyrighted works. Clark Decl. ¶¶ 5(c), (e). When an ad's images and text and the URLs for those are scraped, as here, the ad's contents can also be disaggregated from its creator and used without payment or credit. *Id.* ¶ 5(e). Advertisers have no way of consenting to or preventing the scraping of their data by other users who have installed the UpVoice extension. *Id.* ¶ 5(c), (e). Put differently, although users can view and share ads, they cannot consent to others scraping the ad and adverting metrics in violation of Facebook's Terms of Service. Leathern Decl. ¶ 9.

protected location. *Id.* Facebook automatically generates categories of advertising interests for users based on the user's activities on Facebook, including past engagement with advertising. *Id.*; Leathern Decl. ¶ 6. This information is accessible to users only while securely logged in to their accounts. Leathern Decl. ¶ 6.

C. Defendants Attempted To Evade Facebook's Enforcement Efforts

Facebook has, and continues to, invest substantial resources to detect and stop scraping through technological means, as well as legal means. Clark Decl. ¶¶ 6-7; *see also Stackla, Inc. v. Facebook Inc.*, Case No. 19-cv-05849 (N.D. Cal. 2019); *Facebook, Inc. v. Sluchevsky*, Case No. 19-cv-01277 (N.D. Cal. 2019); *Facebook, Inc. v. Zaghar*, 3:20-CV-04054 (N.D. Cal. 2020).

Here, after an investigation to verify and understand the scope and extent of Defendants' unauthorized scraping, Facebook disabled Defendants' accounts and pages on September 30, 2020. Karve Decl. ¶¶ 5, 28-34. The next day, on October 1, Facebook filed a civil action in state court alleging violations of Facebook's Terms of Service and Instagram's Terms of Use. *See* Mehta Decl. Ex. 2 (Complaint, *Facebook, Inc. v. BrandTotal LTD*, No. 20-CIV-04256 (Cal. Super. Ct.)). Google removed Defendants' extensions from its Chrome Web Store that same day. Karve Decl. ¶¶ 14, 18. On October 3, three days after Facebook disabled defendants' accounts, BrandTotal's Chief Product Officer Oren Dor created an Instagram account in the name of "Jack_Back" and a new Facebook account using the fake name "Jack Busch." *Id.* ¶ 34.[5] Then on October 12, Defendants re-published their UpVoice extension on the Chrome Web Store. *Id.* ¶ 14. It was removed on or about October 14, and then published again that same day. *Id.* Although it now appears to be down (again), the re-published UpVoice extension had been installed at least 150 times after October 14. *Id.*

After learning that Defendants had created Facebook and Instagram accounts using fake names and re-published their extension on the Chrome Web Store, thus evading Facebook's enforcement efforts and accessing Facebook's platform without authorization (again), Facebook voluntarily dismissed its state-court action on October 14, 2020, re-filing this action in federal court to add claims under the CFAA, among others. Declaration of Jason J. Kim ISO Facebook Opp. To TRO ("Kim

[5] Creating a Facebook account using a fake name violates the Facebook Terms. Duffey Decl. Exs. 1, 2 ("[Y]ou must … [u]se the same name that you use in everyday life.").

Decl.") ¶ 8.

II. DEFENDANTS HAVE NOT ESTABLISHED IRREPARABLE INJURY

Defendants seek "an extraordinary and drastic remedy." *Munaf v. Geren*, 553 U.S. 674, 689 (2008). The bar for such relief is high, and Defendants fall far short. To obtain a temporary restraining order, defendants must establish that: (1) they are "likely to succeed on the merits," (2) they are "likely to suffer irreparable harm in the absence of preliminary relief," (3) "the balance of equities tips in [their] favor," and (4) a temporary restraining order "is in the public interest." *Koller v. Brown*, 224 F. Supp. 3d 871, 875 (N.D. Cal. 2016). Moreover, because Defendants seek a ***mandatory*** injunction ordering Facebook to take certain actions, the burden is "doubly demanding." *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015). Such relief "is particularly disfavored," and to be entitled to it, Defendants "must establish that the law and facts ***clearly favor*** [their] position, not simply that [they] are likely to succeed." *Id.*

A. The Requested Relief Would Not Cure The Alleged Irreparable Injury

Defendants seek a TRO compelling Facebook to: (1) "rescind" its "takedown request" to Google and "take other reasonable actions in communication with Google to make the recession [sic] effective so that that UpVoice is again available on the Google Chrome Web Store," (2) "reverse its 'technical enforcement measures' blocking UpVoice from Facebook's platform," and (3) "restore the BrandTotal and other BrandTotal principals Facebook pages." Mem. 25. The requested relief is improper for at least two reasons.

First, Defendants have not satisfied their burden to establish that "the relief sought will actually prevent [the] irreparable harm" alleged. *Sierra Club v. U.S. Dep't of Energy*, 825 F. Supp. 2d 142, 153 (D.D.C. 2011). While Defendants ask Facebook to unblock their Facebook pages and reverse "technical enforcement measures," Defendants have not shown that either would actually solve their supposed problem here. In fact, Facebook's unblocking of their Facebook pages would only allow Defendants to post on Facebook (which they were using to solicit users), not fix the extension; likewise, Facebook is not taking any technical measures that if lifted would allow the extension to work. What Defendants seek—and what they need to repair the purported injury here—is for Google to reinstate the UpVoice extension. But Google is not a party, and Facebook does not control Google.

Indeed, Defendants can only speculate about whether the injunction they seek would accomplish anything. They concede that to obtain the relief sought they "may have to file an action to seek a TRO against Google." Defendants' Response to Plaintiff's Admin. Mtn. to Set Briefing Schedule (Dkt. No. 29) at 3. And they acknowledge that there is no telling how quickly or ***even whether*** Google will respond to any request by Facebook. *Id.* This Court should not enter a mandatory, emergency injunction when the remedy that Defendants need can be provided only by an independent non-party. *See Sierra Club v. U.S. Dep't of Energy*, 825 F. Supp. 2d 142, 153 (D.D.C. 2011) ("It would make little sense for a court to conclude that a plaintiff has shown irreparable harm when the relief sought would not actually remedy that harm …. The inquiry must be whether the plaintiff has shown that the relief sought will actually prevent irreparable harm.").

Second, injunctive relief must be "specific[]" and "precise[]." The relief sought would not be. Defendants request an injunction compelling Facebook, by threat of contempt, to "take other reasonable actions in communication with Google to make the recession effective so that UpVoice is again available on the Google Chrome Web Store." Mem. 25. The requested relief does not "state its terms specifically" nor "describe in reasonable detail … the act or acts restrained or required," as is required of any injunction issued by this Court. Fed. R. Civ. P 65(d). Nor does it provide Facebook with "fair and precisely drawn notice of what the injunction actually [requires]." *Fortyune v. American Multi-Cinema, Inc.*, 364 F.3d 1075, 1086-87 (9th Cir. 2004). It does not, for example, define what would be reasonable, what precisely would be required to make the rescission effective, or what would happen if, despite Facebook's best efforts, Google simply refused to make the UpVoice extension available again. Such a vague and open-ended injunction is impermissible under Rule 65.

B. Even If The TRO Were Not Futile, Defendants Have Not Established That They Are Entitled To Extraordinary Relief

1. Defendants Have Not Shown That They Face An Imminent Risk Of Harm

As Defendants acknowledge, "[a]n adequate showing of irreparable harm is the 'single most important prerequisite for the issuance of a [TRO].'" *Koller*, 224 F. Supp. 3d at 879 (alteration in original) (quoting *Freedom Holdings, Inc. v. Spitzer*, 408 F.3d 112, 114 (2d Cir. 2005)); *see also* Doc.

26-3 at 23. Yet they fall far short of the necessary showing. Mere allegations and speculation are insufficient. *See Stackla, Inc. v. Facebook*, 2019 WL 4738288, at *3 (N.D. Cal. Sept. 27, 2019). Rather, Defendants must "***demonstrate*** immediate threatened injury." *Caribbean Marine Servs. Co. v. Baldridge*, 844 F.2d 668, 674 (9th Cir. 1988). Defendants claim they face the threat of being driven out of business and of losing customers, Mem. 23, but do not sufficiently demonstrate any immediate threat of irreparable harm.

Defendants' CEO avers that, [redacted] Leibovich Decl. ¶ 62. But absent *any* supporting financial information or any evidence of *when* it will be forced to cease operations, such vague and conclusory assertions are insufficient. *See Stackla*, 2019 WL 4738288, at *5 (collecting cases). In *Stackla*, much as here, a content-scraping software company claimed it would go out of business without access to Facebook's platform, relying on the statements of its CEO that the company would "be deprived of its revenue" and "soon reach a tipping point where [it] c[ould] no longer operate." *Id.* at *1, 5. But, without actual evidence of its "financial strength or the likelihood that [it] w[ould] dissolve … at any particular point in time," Chief Judge Hamilton rejected the claim as "inherently speculative." *Id.* at 5; *see also Int'l Medcom, Inc. v. S.E. Int'l, Inc.*, 2015 WL 7753267, at *3, 5 (N.D. Cal. Dec. 2, 2015) (similar). Here, Defendants failure to provide any financial information showing imminent injury is unsurprising. ***Just last month***, BrandTotal procured $12 million in Series B venture capital funding. *BrandTotal Raises $12 Million In Series B Round To Expand Brand Marketing Analytics Technology*, PRNEWSWIRE (Sept. 14, 2020), https://www.prnewswire.com/news-releases/brandtotal-raises-12-million-in-series-b-round-to-expand-brand-marketing-analytics-technology-301130281.html. And in any event, Defendants also scrape data from social-media sites other than Facebook, including YouTube, Twitter, and Amazon, Leibovich Decl. ¶ 6, but they fail to show why those other data sources would not allow them to provide services to their customers. *See Stackla, Inc.*, 2019 WL 4738288, at *TK (finding Stackla has established that "much … of the work [Stackla] conducted for clients … involved accessing Facebook's platforms," but still finding no irreparable injury).

Nor have Defendants demonstrated that they face irreparable harm from losing customers. [redacted]

[redacted] Defendants have not identified any current or prospective customers who have canceled existing contracts or stated that they will not do business with Defendants. Whether these concerns and internal discussions will actually result in lost business is purely speculative, and therefore insufficient to establish irreparable harm. *See Stackla, Inc.*, 2019 WL 4738288, at *4 ("the fact that customers have 'raised … concerns' … does not demonstrate a likelihood that they will cease paying Stackla under the terms of their contracts—much less that they will do so imminently"); *id.* at *4 (rejecting potential loss of prospective customers in part because "Stackla merely alleges but does not demonstrate that Facebook's ban caused this alleged harm (rather than, for example, prior negative media attention), or that the injunctive relief it seeks would be effective in curing it.")). Moreover, any resulting harms from lost customers "are measurable and are best characterized as economic harms" that can be remedied through damages. *Ebates Performance Mktg., Inc. v. Integral Techs., Inc.*, 2013 WL 75929, at *2 (N.D. Cal. 2013). Indeed, Defendants have quantified the harm, claiming that they have lost [redacted]

And in any event, "self-inflicted wounds" and "harm that results from the express terms of [a] contract" are not generally considered irreparable. *Epic Games, Inc. v. Apple Inc.*, 2020 WL 5073937, at *3 (N.D. Cal. Aug. 24, 2020). Facebook's terms expressly prohibit the use of automated means to collect data. Duffey Decl. Exs. 1, 2. Defendants built a business around violating those terms. They should not now be granted extraordinary relief from their very ordinary enforcement.

2. The Timing Of The TRO Request Confirms There Is No Emergency Here

Facebook disabled Defendants' Facebook and Instagram accounts and pages over two weeks ago, around September 30, 2020. Compl. ¶ 58; *see also* Mem. 1 (Facebook disabled Defendants' accounts "[a]pproximately two weeks ago"). Google removed the UpVoice extension from the Google Chrome Web Store on October 1, 2020. Kim Decl. ¶ 2. Yet it was not until October 8, 2020 that Defendants first mentioned that they might seek injunctive relief, and even then, Defendants stated they were planning to wait until the following week to file their request, ultimately filing on October

16, 2020. Kim Decl. ¶¶ 3, 4.[6] Defendants claims that they are at risk of "immense" harm and stand "on the brink of collapse," Mem. 23, cannot be squared with their delay in seeking relief. *Royalty Ambulance Servs. v. HHS*, 2014 U.S. Dist. LEXIS 64000, at *8-9 (C.D. Cal. May 8, 2014) (ten day delay "negates" assertion of irreparable harm). Combined with the other defects set forth above, Defendants' delay confirms that emergency relief is not needed or appropriate.

III. DEFENDANTS ARE NOT LIKELY TO SUCCEED ON THE MERITS

A. Defendants Have Not Shown A Likelihood Of Success On The Merits Of Even Their Own Counterclaims

1. Defendants' Intentional Interference Claims Fail

Defendants have not even adequately pled, let alone shown a likelihood of success on the merits, of their claims for intentional interference with contract and prospective economic advantage.

First, Defendants have not shown that Facebook had "knowledge of [Defendants'] contracts," *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 55 (1998), or knew about "specific economic relationships with identifiable third parties," *Buxton v. Eagle Test Sys. Inc.*, 2010 WL 1240749, at *2 (N.D. Cal. Mar. 26, 2010). Although a declarant [redacted] Leibovich Decl. ¶¶ 39-42, Defendants never identify any *specific* contract or potential relationship with which Facebook ***knowingly*** interfered. This omission is fatal. *Davis v. Nadrich*, 174 Cal. App. 4th 1, 11 (2009) (interference with contract); *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1164-1165 (2003) (prospective economic advantage). Moreover, having failed to establish Facebook's knowledge of any specific contracts or prospective business deals, Defendants have also necessarily failed to establish the separate requirement that Facebook have known that interference with those unknown contracts or prospective deals was "certain or substantially certain to occur as a result" of Facebook's actions. *Korea Supply,* 29 Cal. 4th at 1165 (interference with prospective economic advantage); *Quelimane*, 19 Cal. 4th at 56 (interference with contract).

[6] Facebook did not delay the filing of Defendants' motion. *See* Kim Decl. ¶¶ 3-7. But even if Facebook caused the two-day delay that Defendants complain about, Defendants had already planned to wait roughly ***two weeks*** to file this motion. *Id.* ¶¶ 2, 3.

Second, Defendants have not "demonstrated ***actual breach or disruption*** of the contractual relationship." *Quelimane*, 19 Cal. 4th at 55. Defendants have not demonstrated that any of their existing contracts have been cancelled or even that they were contractually obligated to provide data scraped from Facebook in particular, as opposed to any other website. Rather, they have merely stated [redacted] Leibovich Decl. ¶¶ 34-35.

Third, Facebook acted with a "legitimate business purpose which justified its actions." *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 57 (1998); *see also A. F. Arnold & Co. v. Pacific Professional Ins., Inc.*, 27 Cal. App. 3d 710, 714 (1972). Facebook sought to enforce its terms of service, to which Defendants (and every user whose data they scraped) had agreed. Clark Decl. ¶ 7; Duffey Decl. ¶¶ 3, 4; Karve Decl. ¶¶ 27-34. Even if Defendants were somehow correct that Facebook interfered with their contracts or prospective relationships (they are not), Facebook was entirely justified in incidentally interfering with a contract that threatened "a prior contract of [its] own." *Richardson v. La Rancherita*, 98 Cal. App. 3d 73, 81 (1979) (quoting Prosser on Torts 944-945 (4th ed. 1971)).

Indeed, every action Facebook took was meant to enforce its own contractual agreements and protect its users. Facebook, and the public writ large, have a "strong interest in the integrity of Facebook's platforms" and in safeguarding users' privacy against this scraping. *See Stackla*, 2019 WL 4738288 at *6. And the consistent enforcement of Facebook's anti-scraping policy is essential to maintaining the security and operation of Facebook's network and, by extension, protecting its users. Clark Decl. ¶¶ 5(a), (f). Facebook's efforts to protect user privacy are not the type of "wrongful and malicious" intention that courts require for intentional interference claims. *A. F. Arnold & Co. v. Pacific Professional Ins., Inc.*, 27 Cal. App. 3d 710, 716 (1972) (quoting Prosser on Torts 952-953 (4th ed. 1971)).[7]

[7] Defendants also cannot show that Facebook "engaged in an independently wrongful act," which is required to make out a claim for intentional interference with economic advantage. *Ixchel Pharma, LLC v. Biogen, Inc.*, 9 Cal. 5th 1130, 1142 (2020). An independently wrongful act is one that

Fourth, in all events, Defendants have not demonstrated "that the economic harm it suffered was proximately caused by" Facebook's allegedly wrongful acts. *Korea Supply*, 29 Cal. 4th 1134 at 1165-1166 (prospective economic advantage); *Dryden v. Tri-Valley Growers*, 65 Cal. App. 3d 990, 995-996 (1977) (party must have "caused the breach of contract"). Facebook removed Defendants' accounts and Pages from its platform and sent takedown notices to Google. Leibovich Decl. ¶¶ 19, 22. Defendants have not introduced any evidence that any alleged economic harm was proximately caused by Facebook's actions, as opposed to the removal of the extension from the Google Chrome Web Store.

2. Defendants' Unfair Competition Claims Are Meritless

Defendants allege that Facebook engaged in the three types of wrongful conduct prohibited by the California Business and Professions Code § 17200, *et seq.* ("UCL"): "unlawful" business acts or practice, "unfair" business acts or practice, and "fraudulent" business acts or practice. *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). Defendants have not adequately pled these claims, let alone established they will likely prove them, which is their burden.

Unlawful Prong. Defendants allege that Facebook's "disruption of [Defendants'] contractual and prospective business relationships is unlawful and thus a violation of the UCL." Mem. 20. But Defendants have not established that Facebook's enforcement of its anti-scraping policies—itself a legitimate business practice—constitutes a violation of any predicate for a UCL claim. *See, e.g.*, *Milman v. FCA U.S., LLC*, 2019 WL 3334612, at *8 (C.D. Cal. Apr. 15, 2019) (UCL's unlawful prong failed where all pled underlying crimes and torts failed). Because Defendants cannot establish a likelihood of prevailing on any of its business tort claims, this derivative claim must also fail. *See Nat'l Rural Telecommunications Co-op. v. DIRECTV, Inc.*, 319 F. Supp. 2d 1059, 1074 (C.D. Cal. 2003) (UCL claim premised on "unlawful" action cannot stand "independent of any law"). Indeed, contrary to being unlawful, the FTC consent decree that Defendants cite obligates Facebook to report scraping incidents.

Unfair Prong. Defendants also assert that Facebook's actions are unfair business practices

---

is "unlawful," meaning "proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard." *Korea Supply*, 29 Cal. 4th at 1159.

because they were denied access to Facebook's platforms. Mem. 21. Because Defendants claim injury as direct competitors of Facebook, Mem. 21, the "unfair" prong requires them to establish that Facebook's conduct "threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel-Tech*, 20 Cal. 4th at 187.

Defendants do not come close to satisfying this standard. Defendants appear to advance two theories: (1) "Facebook is unlawfully unfairly leveraging its power in the social networking market to secure an anticompetitive advantage in the data analytics market" and (2) Facebook is denying Defendants access to "a facility it controls that is essential to its competitors." Mem. 21-22. The first theory is not cognizable because the Ninth Circuit has expressly rejected "a monopoly leveraging doctrine as an independent theory of liability." *Alaska Airlines, Inc. v. United Airlines, Inc.*, 948 F.2d 536, 541 (9th Cir. 1991); *see also hiQ Labs, Inc. v. LinkedIn Corp.*, 2020 WL 5408210, at *12 (N.D. Cal. Sept. 9, 2020) ("[A]n antitrust violation requires that there be anticompetitive conduct and leveraging by itself is not inherently anticompetitive in nature.").

Defendants' second theory, that Facebook is denying access to an "essential facility" fails for multiple reasons including the threshold problem that Defendants acknowledge that Facebook does not control whether a browser extension is permitted or removed from the Google Chrome Web Store. *See MetroNet Servs. Corp. v. Qwest Corp.*, 383 F.3d 1124 (9th Cir. 2004) (stating that essential facilities claim requires plaintiff to show "*defendant* has refused to provide plaintiff access to the facility").

The Ninth Circuit has rejected UCL claims where a violation of the "spirit" of antitrust laws is alleged, Mem. 21, without a cognizable antitrust violation. *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1136-37 (9th Cir. 2014) (plaintiff's general UCL allegations did not suffice to allege what "amounts to a violation of antitrust laws."). But even looking just at the "spirit" of Defendants' claims, they still fall well short. Defendants' theories boil down to a claim of "forced sharing," but the Supreme Court has cautioned against forcing such arrangements "because of the uncertain virtue of forced sharing and the difficulty of identifying and remedying anticompetitive conduct by a single firm." *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 407 (2004).

Fraudulent Prong. Defendants next allege that Facebook's terms were "fraudulent" because they "promise … users that only the users own their content." Mem. 22-23. "But a business practice is fraudulent only if 'members of the public are likely deceived.'" *Nat'l Rural Telecommunications Co-op.*, 319 F. Supp. 2d at 1077. And those same terms expressly state that users shall "[n]ot share your password, give access to your Facebook account to others, or transfer your account to anyone else (without our permission)." Duffey Decl. Ex. 1. They also state that users "may not access or collect data from [Facebook's] Products using automated means (without [Facebook's] prior permission) or attempt to access data [users] do not have permission to access." Duffey Decl. Ex. 1. In light of those express provisions, there was no deception to dispel because no reasonable user would understand the Facebook terms to mean that a user has the power to grant a third-party access to Facebook's computer network. Facebook's terms expressly prohibit users from engaging in precisely the conduct Defendants admit. *See, e.g.*, *Ebner v. Fresh, Inc.*, 838 F.3d 958, 966 (9th Cir. 2016) (concluding that disclosure defeated a claim under UCL's fraud prong). Defendants' UCL claim is unlikely to succeed on the merits.[8]

[8] Even if Defendants were somehow to make out a claim for intentional interference or under the UCL for removing Defendants' Facebook accounts and Pages, their claims would be barred under 47 U.S.C. § 230(c)(1) because they seek to impose liability on Facebook for declining to publish Defendants' content. *See, e.g., Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 110 (9th Cir. 2009) (laying out test). *First*, Facebook is an "interactive computer service," in that it "provides or enables computer access by multiple users to a computer serv[er]." *See Sikhs for Justice, v. Facebook, Inc.*, 144 F. Supp. 3d 1088, 1093 (N.D. Cal. 2015), *aff'd* 697 F. App'x 526 (9th Cir. 2017). *Second*, Defendants' browser extension and accounts and pages constitutes "information created by another information content provider" because Facebook had no hand in their creation and a computer program like a browser extension or a Facebook page are forms of information. *See Sikhs for Justice*, 144 F. Supp. 3d at 1093 (Facebook page); *Intango, Ltd. v. Mozilla Corp.*, No. 20-cv-02688 (N.D. Cal. Aug. 17, 2020), Dkt. 41-3 at 2, 6 (holding that "web extensions, or 'add-ons,' for web browsers" qualify under this prong). Finally, Defendants' claims (as they describe them) all involve Facebook's decision "whether to publish or to withdraw from publication third-party content"—i.e., Facebook's enforcement of its anti-scraping policies. *See Barnes*, 570 F.3d at 1102; *see also* Answer ¶¶ 46, 60; Mem. 19 (alleging Facebook "revok[ed] BrandTotal's access to UpVoice user information").

B. Defendants Are Not Likely To Succeed On Facebook's Claims

1. Facebook Will Succeed On Its Breach Of Contract Claim

a. Defendants Breached Facebook's Terms Of Service By Collecting User Data Via An Automated Browser Extension

Defendants do not dispute that three of the four elements for breach of contract—i.e., that there is a contract, Facebook complied with its obligations, and Facebook suffered damages—are satisfied here. Mem. at 9-10; *see also* Answer ¶ 46; Duffey Decl. Ex. 1-4; Clark Decl. ¶¶ 5(b), (f); *see generally E.D.C. Techs. v. Seidel*, 216 F. Supp. 3d 1012, 1015 (N.D. Cal. 2016) (elements of breach of contract). The only dispute here is whether Defendants breached. And even there, there really is no legitimate dispute.

Defendants violated at least three separate provisions of Facebook's terms: (1) they violated 3.2.1 by behaving in an "unlawful, misleading or fraudulent manner" (e.g., suggesting to Defendants' customers that Facebook was "participat[ing]" in Defendants' data scraping, entering password protected locations on Facebook's platform pretending to be an authenticated user); (2) they violated 3.2.2 by "doing [some]thing that could … impair the proper working or appearance of [Facebook] products" (e.g., interfering with the normal operation of Facebook's network and security operations); and (3) they violated 3.2.3 by "access[ing] or collect[ing] data from [Facebook] Products using automated means (without [Facebook's] permission)," (via the UpVoice extension). *See* Duffey Decl. Ex. 1-4; *see generally* Karve Decl.

Defendants do not even argue that they did not breach Facebook Terms 3.2.1 (misleading or fraudulent behavior) and 3.2.2 (impairing the appearance/working of a Facebook product). That is reason alone to deny the TRO. As to the third breach, Defendants' only response is that they did not access or collect data using "automated means." They argue that (a) they have users' consent to collect users' information, (b) they are not engaging in "controversial" behavior, like collecting information on undecided voters in the run up to an election, and (c) they have not automatically installed their browser extension on Facebook users' computers. *See* Mem. 10.[9] Not one of these points, however, is

[9] Defendants also assert that they did not breach *Instagram's* Terms because they have "the users' permission for the data [they] collect[]." Mem. 9-10. This is wrong. Not only do Defendants

relevant to the question of whether, once installed, Defendants' browser extension used "automated means" to extract data from Facebook's protected computers. *See* Cal. Civ. Code § 1638 ("The language of a contract is to govern its interpretation, if the language is clear and explicit."). Facebook, on the other hand, has presented sworn statements that UpVoice does employ automated data scraping. *See* Karve Decl. ¶ 13, 15-16; Clark Decl. ¶ 14. Indeed, Defendants ***admit*** elsewhere in its TRO briefing that UpVoice automatically collects information both from those who download it and from the advertising that a user sees. *See, e.g.*, Mem. 11 (UpVoice uses "some degree of automation" to collect information).

b. Defendants' Novel Argument That A Contractual Provision Barring Data Scraping On A Private Website Violates Public Policy Is Meritless

Unable to meaningfully dispute that they breached their contracts with Facebook, Defendants ask the Court to find, ***on a TRO no less***, that they are likely to succeed on their claim that important provisions of Facebook's terms of service should be invalidated as a matter of public policy. The argument is both (a) unresponsive to two of Facebook's theories of breach and (b) wrong.

To be clear, Facebook's terms do not bar individual users from collecting their own data, as Defendants concede. *See* Mem. 16 (asserting that "Facebook's Terms … do not prohibit a user from manually collecting the same data BrandTotal collects through UpVoice"). Facebook affirmatively enables each user to download their information and take it to another platform. *See, e.g.*, Erin Egan, *It's Time To Make Our Privacy Materials Easier To Find* (Mar. 28, 2018), https://about.fb.com/news/2018/03/privacy-shortcuts/. Term 3.2.3, in contrast, bars automated collection of data by a third-party. *See supra* p. 5. It also prohibits misleading statements like those made by Defendants suggesting that Facebook approved of—and perhaps even oversaw—Defendants' actions. *See* Compl. ¶ 50 & Exs. 6, 11, 13.[10] Ultimately, Term 3.2.3 protects the integrity of the

not have users' informed consent, but their scraper picks up information from a wide array of individuals who have not agreed to have their information snatched up. *See supra* pp. 6-7.

[10] Facebook sent a cease and desist letter to Unimania on February 14, 2020, requesting that it cease use of Instagram's trademark in connection with its extensions. *See* Mehta Decl. Ex. 3.

platform and the information of all users that engage there. For example, from a security perspective, Defendants' method of scraping—through logged-in users' accounts—is not dissimilar to methods used by hackers who improperly access accounts based on stolen or phished credentials and exfiltrate data without user consent. Facebook's systems cannot detect whether a user has consented off-platform to a third party—such as Defendants—exfiltrating data from the users' account and therefore cannot just allow third parties to scrape up data through these means.

Against this backdrop, Defendants' misguided belief that their novel arguments for an unenumerated property right in user data (based on a misreading of the CCPA[11]) are so strong that they have a clear likelihood of success in invalidating Facebook's terms of service is neither credible nor legally supported.[12] Likewise, Defendants are wrong that Term 3.2.3 has been used to "improperly stamp[] out competition." As explained, Term 3.2.3 is not about competition at all; it prohibits unauthorized collection of data by third-parties. Scraping can be harmful for any number of reasons. *See* Clark Decl. ¶ 5. And Defendants' business model implicates many of these concerns. *See* Compl. Ex. 12 at ¶¶ 5.4-5.5.

This Court should reject the illogical argument—developed only after Defendants were caught improperly accessing Facebook's users' data—that allegations about Facebook's past user privacy practices somehow bar it from taking steps to protect user data. If anything, "Facebook's recent interactions with the FTC" only underscore "[t]he public['s]strong interest in the integrity of Facebook's platforms, Facebook's policing of those platforms for abuses, and Facebook's protection of its users' privacy." *Stackla*, 2019 WL 4738288 at *6.

---

[11] Defendants do not point to a single provision giving rights to data scrapers to collect and monetize data. The statements of Assembly member Edwin Chau do not change this calculus; he merely said that the CCPA gives consumers "more control over their data." Mem. 11-12; *see also Garcia v. United States*, 469 U.S. 70, 76 (1984) (cautioning against reliance on "passing comments" in interpreting a statute).

[12] As explained, the *HiQ* case is also wholly inapposite. *See infra* pp. 22-23. Indeed, *HiQ* acknowledged that even though the data scraper's actions did not fall under the CFAA, "victims of data scraping" could bring a "breach of contract" action instead. 938 F.3d at 1004. Invoking *HiQ* against a cause of action that the decision encouraged litigants to consider makes little sense.

2. Facebook Will Prevail On Its CFAA and Section 502(c) Claims

In its complaint, Facebook alleged Defendants' post-revocation conduct violated the CFAA and California Penal Code, § 502(c). Compl., ¶¶ 81-95. Facebook alleges Defendants violated section 1030(a)(2) of the CFAA because, after Facebook revoked Defendants' access to Facebook, Defendants published the UpVoice extension on the Google Chrome Web Store and used it to access and scrape Facebook computers. Compl., ¶ 84. The complaint also alleges Defendants violated section 1030(a)(4) because they used fraud to send unauthorized commands and requests to Facebook computers, concealed as requests from an authenticated user. *Id.,* ¶ 85. Defendants' post-revocation conduct also serves as the basis for the violation of California Penal Code, § 502. Compl., ¶¶ 87-95. Facebook's section 502 claims allege Defendants accessed, used, and copied data from Facebook's computers without Facebook's permission. *Id.*

This case is consistent with *Power Ventures*. There, Power Ventures operated a website extracting and aggregating users' social networking information from Facebook and other social networking sites onto a single page. *Facebook, Inc. v. Power Ventures*, 844 F.3d 1058, 1062 (9th Cir. 2016). Facebook sent a cease and desist letter to Power Ventures, explicitly revoking any authorization that Defendants may have believed they had to access password-protected locations on Facebook's site. The Ninth Circuit held that Power Ventures had violated the CFAA because it continued to access password-protected Facebook member profiles after Facebook's "express revocation of permission." *Id.* at 1068. Here, Facebook disabled the Defendants' accounts and Pages and filed a civil action against Defendants in the Superior Court of California alleging violations of Facebook and Instagram's Terms based on Defendants' scraping activity. Karve Decl. ¶¶ 27-34; Mehta Decl. Ex. 2. After the complaint was filed, and after Google removed the extension from its Web Store, Defendants re-published a functionally identical version of the UpVoice extension. Karve Decl. ¶¶ 14, 16. Like the defendant in *Power Ventures*, Facebook's civil action put Defendants "on notice that [they were] no longer authorized to access Facebook's computers" yet they proceeded to "deliberately disregard[]" that notice. *Power Ventures*, 844 F.3d at 1067-1068 & n.3. *Power Ventures* holds that Defendants' post-revocation conduct in this case violates the CFAA. *Id*.

Ignoring *Power Ventures* entirely, Defendants contend this case is "nearly identical" to *hiQ*

Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). Mem. 9. But they miss the premise of that decision. The CFAA's prohibition on unauthorized access applies fully to "information delineated as *private* through use of a permission requirement … such as password authentication." 938 F.3d at 1001. Because hiQ was scraping non-password protected member profiles from a publicly-accessible location on LinkedIn's website, the Ninth Circuit reasoned that CFAA's prohibition on accessing a computer "without authorization" likely did not apply. *Id.* at 990-991, 1003. The Ninth Circuit explicitly distinguished the password protection in *Power Ventures*: Power Ventures ran afoul of the CFAA because it "was gathering user data that was protected by Facebook's username and password authentication system." *hiQ*, 938 F.3d at 1002 (citing *Power Ventures*, 844 F.3d at 1063); *see also United States v. Nosal* (*Nosal II*), 844 F.3d 1024 (9th Cir. 2016) (holding former employee who used current employee's login credentials to access company's computers and collect information acted "without authorization" under CFAA). "In sum *Nosal II* and *Power Ventures*"—and not *hiQ*—"control situations in which authorization generally is required and has either never been given or has been revoked." *hiQ*, 938 F.3d 1002. That is precisely the situation here—Defendants are scraping information from password-protected locations on Facebook, only accessible to authenticated users. According to *hiQ* itself, *Power Ventures* delineates the CFAA's framework for the scraping at issue here. *See hiQ*, 938 F.3d at 1002.

Contrary to Defendants' suggestion, the fact that users may have consented to the installation of a browser extension does not transform Facebook's computer network into the type of publicly-available website at issue in *hiQ*. Assuming user consent is relevant, user consent only gets Defendants so far. In *Power Ventures*, Facebook users who signed up for Power Ventures purported to give Power Ventures permission to disseminate messages through the Facebook system. *Id.* at 1067. But Facebook "expressly rescinded" any purported permission with a cease and desist letter to Power Ventures, and therefore, "[t]he consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." *Id.* at 1067-68. "[F]or Power to continue ... using Facebook's computers, it needed authorization *both* from individual Facebook users (who controlled their data and personal pages) *and* from Facebook (which stored this data on its physical servers)." *Id.* at 1068. So too here.

Ultimately, because Defendants' affirmative state-law claims are premised on their ability to engage in conduct that violates the CFAA, the Court cannot grant the relief Defendants' seek as it would "stand as an obstacle to the accomplishment … of the full purposes and objectives of [federal]" law. *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372-373 (2000); *see also Hathorn v. Lovorn*, 457 U.S. 255, 270 (1982) (courts must "refrain from ordering relief that would violate federal law").

3. Facebook Is Likely To Succeed On Its Interference With Contract Claim

Defendants barely try to rebut Facebook's allegations that they interfered with Facebook's contractual relations. Defendants claim there was no interference because they have never asked Facebook users for their passwords. Dor Decl. ¶ 16. This ignores that users ***also*** agreed not to "access or collect data … using automated means" or "give access to [their] Facebook account to others." Clark Decl. ¶ 7, Duffey Decl. Ex. 1. Indeed, Defendants' extension does not work without logged-in access to a Facebook user's account. Karve Decl. ¶¶ 13, 15. On this critical point, Defendants have no response at all.

IV. THE BALANCE OF EQUITIES WEIGHS AGAINST EXTRAORDINARY RELIEF

Defendants wrongly assert that the balance of equities weighs in its favor because it purportedly faces extinction if it is not permitted to scrape Facebook's platform and "Facebook suffers no harm" by allowing Defendants to continue to scrape data while the litigation proceeds. Far from it.

An actor with unclean hands has a weak claim to the equities. Defendants made the decision to violate Facebook's terms, and thus are responsible for their dilemma. *See Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 784 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019) (balance of hardships weighed in favor of permanent injunction even though injunction threatened Power Ventures' livelihood). And the issuance of a TRO in this case would not be harmless. It would force Facebook to allow a non-compliant developer back on its platform, and interfere with Facebook's ability to enforce its terms and policies and secure its platform. Clark Decl. ¶¶ 5(a), (f).[13]

[13] Defendants suggest this Court forego a bond if it enters a TRO. While Facebook would be entitled to a bond, it is difficult to know what the amount should be because the harm to Facebook's platform is concrete but difficult to quantify. That is precisely why emergency relief should not be

V. THERE IS NO PUBLIC INTEREST IN PERMITTING ILLEGAL DATA SCRAPING

Defendants wrongly assert that the public has a significant interest in forcing Facebook to reinstate platform access to a third-parties that engaged in impermissible data scraping. Not so. The public interest is better served by permitting Facebook to take all necessary steps to protect user privacy. *See* Clark Decl. Ex. 1. The particular violation of Facebook's terms at issue here, automated data collection of data from password-protected locations, is particularly troubling. Clark Decl. ¶¶ 3, 5. That Facebook is taking affirmative steps to enhance user privacy against bad actors is no doubt in the public interest. *See Stackla, Inc.*, 2019 WL 4738288, at *6 ("Facebook's ability to decisively police the integrity of its platforms is without question a pressing public interest."); *Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019) ("The public has an interest in ensuring that computers are not accessed without authorization."); *Facebook, Inc. v. Sluchevsky*, 2020 WL 5823277, *11 (N.D. Cal. Aug. 28, 2020), *adopted in relevant part*, 2020 WL 5816578 (N.D. Cal. Sept. 20, 2020) (finding cognizable public interest supporting entry of permanent injunction).

Granting Defendants' injunction would have the effect of second-guessing, through a federal civil action, Facebook's considered exercise of its authority to maintain the integrity of its platforms. The ramifications for technology companies and their users would be far-reaching and at odds with the efforts that Facebook and other companies are taking every day to enhance protection for user data.

VI. CONCLUSION

The Court should deny the Plaintiffs' motion for a temporary restraining order.

Dated: October 21, 2020

WILMER CUTLER PICKERING HALE AND DORR LLP

By: */s/ Sonal N. Mehta*
Sonal N. Mehta

Attorney for Plaintiff Facebook, Inc.

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

CERTIFICATE OF SERVICE

I hereby certify that on October 21, 2020, I electronically filed the above document with the Clerk of the Court using CM/ECF which will send electronic notification of such filing to all registered counsel.

Dated: October 21, 2020

By: */s/ Sonal N. Mehta*
Sonal N. Mehta